Dr.WEB®

Anti-virus for Mac OS X

User Manual

DISCLAIMER
In no event shall Doctor Web and its resellers or distributors be liable for errors or omissions, or any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, the use of or inability to use information contained in this document.

Dr.Web® Anti-virus for Mac OS X
Version 6.0.2
User Manual
11.03.2011

Doctor Web Head Office
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

Web site: www.drweb.com
Phone: +7 (495) 789-45-87

Refer to the official web site for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web® information security solutions which provide efficient protection from malicious software and spam.

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards. State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

We thank all our customers for their support and devotion to the Dr.Web products!

Table of Contents

Document Conventions

The following conventions and symbols are used in this manual:

Convention	Description
Bold	Names of buttons and other elements of the graphical user interface (GUI), and required user input that must be entered exactly as given in the guide.
Green and bold	Names of **Dr.Web** products and components.
Green and underlined	Hyperlinks to topics and web pages.
`Monospace`	Code examples, input to the command line and application output.
Italic	Placeholders which represent information that must be supplied by the user. For command-line input, it indicates parameter values. In addition, it may indicate a term in position of a definition.
CAPITAL LETTERS	Names of keys and key sequences.
Plus sign ('+')	Indicates a combination of keys. For example, ALT+F1 means to hold down the ALT key while pressing the F1 key.
Exclamation mark	A warning about potential errors or any other important comment.

The following abbreviations are used in this manual:

- CPU - Central Processing Unit
- GUI - Graphical User Interface
- OS - operating system
- RAM - Random Access Memory

Chapter 1. Introduction

Thank you for purchasing **Dr.Web® Anti-virus for Mac OS X**. It offers reliable protection from various types of computer threats using the most advanced virus detection and neutralization technologies.

This manual is intended to help users of computers running Mac OS install and use **Dr.Web for Mac OS**.

About Dr.Web for Mac OS

Dr.Web for Mac OS is an anti-virus solution designed to help users of computers running Mac OS X protect their machines from viruses and other types of threats.

The core components of the program (*anti-virus engine* and *virus databases*) are not only extremely effective and resource-sparing, but also cross-platform, which allows specialists in **Doctor Web** to create outstanding anti-virus solutions for different operating systems. Components of **Dr.Web for Mac OS** are constantly updated and virus databases are supplemented with new signatures to assure up-to-date protection. Also, a heuristic analyzer is used for additional protection against unknown viruses.

Dr.Web for Mac OS consists of the following components each performing its own set of functions:

Component	Description
Scanner	This virus-detection component is used for: • Express, full and custom system scan on user demand or according to schedule. • Neutralization of detected threats (Cure, Delete, Quarantine). The action is either selected by the user manually, or automatically according to the **Dr.Web for Mac OS** settings for the corresponding type of threat.
SpIDer Guard	This is a resident anti-virus component which checks all files (which are being used) in real time.
Quarantine	This is a special folder which is used for isolation of infected files and other threats so that they cannot do harm to the system.
Updater	This is an automated updating utility that is used for updating virus databases and other program components on user demand or according to schedule.
License Manager	This component is used to simplify management of key files, it allows to receive demo and license key files, view information about them and renew your license.
Scheduler	This component is required to perform system scanning and program updates according to schedule. **Scheduler** remains active even when you quit **Dr.Web for Mac OS**.

Flexible settings of **Dr.Web for Mac OS** allow to adjust sound notifications for various events, maximum size of **Quarantine**, list of files and folders excluded from scanning, etc.

License Key File

Use rights for **Dr.Web for Mac OS** are regulated by a special file called the *key file*. The key file contains the following information:

- Duration of the anti-virus license
- List of components a user is allowed to use
- Other restrictions (for example, the number of users allowed to use the application)

The key file has the .key extension and it can be received at first launch of **Dr.Web for Mac OS** via the License Manager:

- For evaluation purposes you can use a demo key file. The demo key file provides full functionality of the main anti-virus components, but has a limited term of usage.
- To get a license key file, you will need the product's serial number. You can purchase any **Dr.Web** anti-virus product or the serial number for it via our partners or the online store.

The key file is delivered as a file with the .key extension or as a ZIP archive containing such file.

The parameters of the key file which specify the user’s rights are set in accordance with the License agreement. The file also contains information on the user and seller of the anti-virus.

By default, the license key file should be located in the /Library/Application Support/DrWeb/keys/ folder. **Dr.Web for Mac OS** verifies the file regularly. Do not edit or otherwise modify the file to prevent the license from compromise.

When the license key file expires, to continue using **Dr.Web for Mac OS** you have to get a new key file and replace the old one with it (see Obtaining Key Files).

Chapter 2. Installation and Removal

The **Dr.Web® Anti-virus for Mac OS X** software is distributed as a single disk image file (drweb-600-mac.dmg). The file can be found on the product CD/DVD or downloaded via the Internet from the **official Doctor Web Web site** at http://www.drweb.com.

⚠ **Dr.Web for Mac OS** is not compatible with anti-virus software including its own earlier versions. Installing two anti-virus programs on one computer may lead to system crash and loss of important data. If you already have an anti-virus software installed, uninstall it before starting a new anti-virus installation (for instructions on uninstalling **Dr.Web for Mac OS**, see Installing and Removing Anti-virus).

System Requirements

Dr.Web for Mac OS can be installed and run on a computer which meets the following minimum requirements:

Component	Requirement
Processor	Any Intel processor.
Memory	Minimum 64 MB of RAM.
Hard disk space	Minimum 80 MB of disk space for a full installation. More disk space may be required depending on the amount and size of objects in **Quarantine**.
Operating system	Mac OS X 10.4 or later.
Other	Internet connection is required to update **Dr.Web virus databases** and **Dr.Web for Mac OS** components.

Other requirements are similar to those of the operating system.

Installing and Removing Anti-virus

To use **Console Scanner**, ensure that the /usr/local/bin/ folder exists before installing **Dr.Web for Mac OS**. If the folder does not exist, you can create it by executing the following commands in Mac OS Terminal:

```
sudo mkdir /usr/local/bin
sudo chown root:wheel /usr/local/bin
sudo chmod 755 /usr/local/bin
```

To install Dr.Web for Mac OS

1. Mount drweb-600-mac.dmg and start the installation.
2. The welcome window of the **Dr.Web for Mac OS** installer will open. Follow the steps and instructions of the installer.
3. Specify the name and password of any administrator account on your computer. Installation will be performed automatically.

To uninstall Dr.Web for Mac OS

1. Mount drweb-600-mac.dmg.
2. Select **Dr.Web Uninstaller**.
3. Specify the name and password of an administrator account on your computer. **Dr.Web for Mac OS** will be removed automatically.

Obtaining Key Files

After installation, you need to register **Dr.Web for Mac OS** to confirm legitimacy of using the anti-virus and unlock the updating and constant protection features. When you run **Dr.Web for Mac OS** for the first time, registration starts automatically. You can also launch registration from License Manager by clicking **Get new license**.

Select the necessary option and click **Continue**:

Option	Description
Receive license key file	You will need to specify the serial number which is included with the program.
Receive demo key file	No serial number is needed because the demo key file is used for evaluation purposes and has a short term of usage.
I already have a valid key file	Select this option if you already have a valid key file present on the computer.

If you select one of the first two options, you will be asked to specify your personal information (name, e-mail address, country and city of residence). This information is used only by **Doctor Web** to generate the key file and is not passed on to anyone else. The key file which you will receive will contain this information for identification purposes. For more information, see Registering Anti-virus.

By default, the license key file should be located in the installation folder. **Dr.Web for Mac OS** verifies the file regularly. Do not edit or otherwise modify the file to prevent the license from compromise.

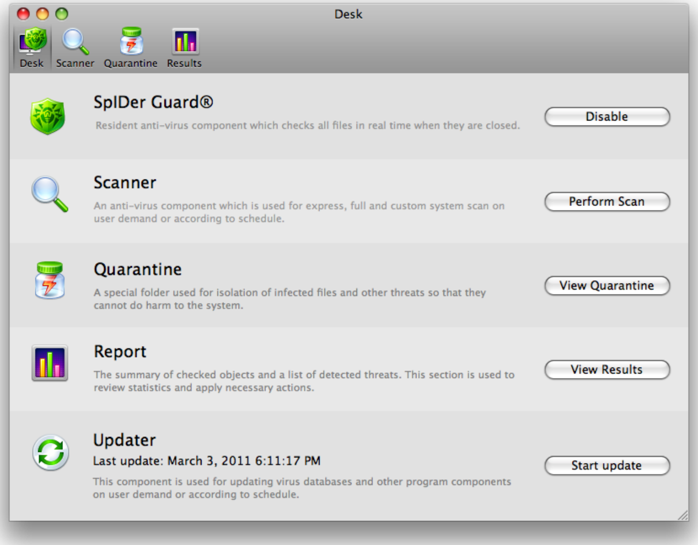
If no valid license or demo key file is found, **Dr.Web for Mac OS** components are blocked. You can access **Updater** only in order to register the product and receive a key file.

Chapter 3. Basic Functions

This chapter contains information on the main functions of **Dr.Web for Mac OS**.

You can access all main functions from the **Dr.Web for Mac OS** window (see picture below). This window consists of sections that helps you control and access anti-virus components:

Section	Descriptions
Desk	In this section, you can: • Enable or disable the **SpIDer Guard** resident anti-virus component. For details, see Constant Anti-virus Protection. • Review information about the last update and start an update manually if necessary. For details, see Updating Anti-virus. • Open the **Scanner**, **Quarantine** or **Results** section.
Scanner	Lets you access the main on-demand anti-virus scanning component. For details, see Scanning System On Demand.
Quarantine	Lets you access and control the contents of **Quarantine**. For details, see Managing Quarantine.
Results	Lets you access and view operation statistics of **Dr.Web for Mac OS** with a summary on detected threats and apply necessary actions. For details, see Viewing Results.



SpIDer Guard®

Resident anti-virus component which checks all files in real time when they are closed.

Scanner

An anti-virus component which is used for express, full and custom system scan on user demand or according to schedule.

Quarantine

A special folder used for isolation of infected files and other threats so that they cannot do harm to the system.

Report

The summary of checked objects and a list of detected threats. This section is used to review statistics and apply necessary actions.

Updater

Last update: March 3, 2011 6:11:17 PM

This component is used for updating virus databases and other program components on user demand or according to schedule.

Picture 1. Main program window.

Starting and Quitting Anti-virus

To start Dr.Web for Mac OS

Do one of the following:

- In the Finder, open the **Application** folder and double-click **Dr.Web for Mac OS**.
- Click the **Dr.Web for Mac OS** icon in the menu bar and select **Open Dr.Web**.

To quit Dr.Web for Mac OS

- Click the **Quit Dr.Web for Mac OS** item in the application menu (the menu bar is at the top of the main desktop).
- Press COMMAND+Q on the keyboard when **Dr.Web for Mac OS** is active.

When you quit **Dr.Web for Mac OS**, **SpIDer Guard** and **Scheduler** remain active. The former is a resident anti-virus monitor which checks all files in real time when they are used, and the latter starts the scanning and updating processes according to schedule (see Configuring Schedules).

Updating Anti-virus

New types of computer threats with new concealment features are being constantly developed by malefactors all over the world. Updating the components and virus databases of **Dr.Web for Mac OS** ensures that your protection is always up to date and ready for those new threat types. Updating is performed by a special component called **Updater**.

You can periodically start **Updater** manually (see below) or configure **Scheduler** to update program components and virus databases according to a specified schedule (see Configuring Schedules).

To start Updater manually

Do one of the following

- In the **Updater** section of the **Dr.Web for Mac OS** main window, click **Update**.
- Click the **Dr.Web for Mac OS** icon in the menu bar and select **Update**.

Constant Anti-virus Protection

Constant anti-virus protection is carried out via a resident component called **SpIDer Guard** that checks all files accessed by the user or other programs in the system in real time. By default, it is enabled as soon as you install and register **Dr.Web for Mac OS**. Whenever a threat is detected, **SpIDer Guard** displays a warning and applies actions according to the anti-virus preferences (see Configuring Automatic Actions).

To enable or disable SpIDer Guard

Do one of the following

- In the **SpIDer Guard** section of the main window, click **Enable** or **Disable**.
- On the menu bar, click the **Dr.Web for Mac OS** icon and select the corresponding item.

Only users with administrator privileges can disable **SpIDer Guard**.

Be extremely cautious when using this option! While **SpIDer Guard** functions are disabled, avoid connecting to the Internet and check all removable media using **Scanner** before accessing.

You can exclude certain files and folders from scanning by **SpIDer Guard** and set up the maximum time for scanning one file in the anti-virus preferences (see Excluding Files from Scanning).

Scanning System On Demand

On-demand scanning is performed by **Scanner**. It checks objects in the file system on your demand or according to a schedule and detects various threats that may be present in the system though inactive. It is necessary to run a system scan periodically using the **Scanner** section of the **Dr.Web for Mac OS** window.

You can start scanning manually (see below) or configure **Scheduler** to scan the system according to a specified schedule (see Configuring Schedules).

Process load increases during scanning which may lead to rapid discharge of batteries. We recommend starting scans when portable computers are powered by mains electricity.

To scan system manually

1. Open the **Scanner** section of the **Dr.Web for Mac OS** window.
2. Select a scan mode (for details, see the file system pane):
   - **Express scan** – run a quick check of the most vulnerable parts of the system only.
   - **Full scan** – perform a full scan of the entire file system.
   - **Custom scan** – manually specify files and folders that you want to check.
   - **User scan** (if added) – check previously specified files and folders.

   The first three modes are present by default. They are also called "scan sets" because they contain information about sets of objects to be scanned. You can create user scan modes. To add a new mode, click the + button under the list of scan modes and name the mode. You can create as many additional scan sets as you want and delete those that you do not need by selecting them and clicking the − button under the list of scan modes.

3. If you chose a **Custom scan** or user scan mode, select checkboxes next to the files and folders that you want to scan.

   You can add other objects to the scan by clicking the + button under the list of scan objects. To delete an object that you do not need, select the object and click the − button under the list of scan objects. When configuring a user scan mode, all settings are saved and then restored when you select the mode again (unlike when using the **Custom scan** mode).

4. Click the ⚙▾ button to select how to apply actions for detected threats. When automatic reaction is enabled, **Scanner** applies actions automatically as specified in the anti-virus preferences. By default, **Scanner** allows you to select necessary action manually for each detected threat.
5. In the bottom right part of the **Scanner** section, click **Start**.

When you start scanning, the main window switches to the **Results** section (see Viewing Results) and virus databases begin loading. **Scanner** displays the name of each file that is currently being scanned and populates the list of detected threats.

Scanner requires administrator privileges to check critical areas of the hard drive. To grant **Scanner** administrator privileges for every scanning process, click the icon of a lock at the bottom of the **Scanner** section and enter administrative password.

Getting Help

To get help about the program you can use **Dr.Web Help** which can be accessed via the Apple Help viewer.

To access Dr.Web Help

In the menu bar, click **Help** and select **Dr.Web Help**, or search for keywords using the text box.

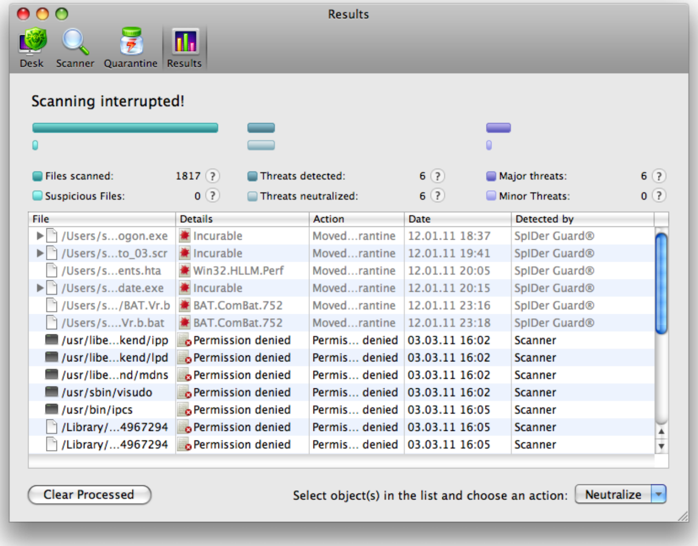
If you cannot find a solution for your problem or necessary information about **Dr.Web for Mac OS**, you can request direct assistance from Technical Support.

Chapter 4. Advanced Use

This chapter contains information on performing more advanced tasks with **Dr.Web for Mac OS** and adjusting its settings.

Viewing Results

The **Results** section (see picture below) of the main windows displays statistic summary of the latest or current scanning session. During scanning, this section also displays the name of the file that is currently being scanned and command buttons.



Scanning interrupted!

Files scanned: 1817
Suspicious Files: 0
Threats detected: 6
Threats neutralized: 6
Major threats: 6
Minor Threats: 0

File	Details	Action	Date	Detected by
/Users/s...ogon.exe	Incurable	Moved...rantine	12.01.11 18:37	SpIDer Guard®
/Users/s...to_03.scr	Incurable	Moved...rantine	12.01.11 19:41	SpIDer Guard®
/Users/s...ents.hta	Win32.HLLM.Perf	Moved...rantine	12.01.11 20:05	SpIDer Guard®
/Users/s...date.exe	Incurable	Moved...rantine	12.01.11 20:15	SpIDer Guard®
/Users/s.../BAT.Vr.b	BAT.ComBat.752	Moved...rantine	12.01.11 23:16	SpIDer Guard®
/Users/s....Vr.b.bat	BAT.ComBat.752	Moved...rantine	12.01.11 23:18	SpIDer Guard®
/usr/libe...kend/ipp	Permission denied	Permis... denied	03.03.11 16:02	Scanner
/usr/libe...kend/lpd	Permission denied	Permis... denied	03.03.11 16:02	Scanner
/usr/libe...nd/mdns	Permission denied	Permis... denied	03.03.11 16:02	Scanner
/usr/sbin/visudo	Permission denied	Permis... denied	03.03.11 16:02	Scanner
/usr/bin/ipcs	Permission denied	Permis... denied	03.03.11 16:05	Scanner
/Library/...4967294	Permission denied	Permis... denied	03.03.11 16:05	Scanner
/Library/...4967294	Permission denied	Permis... denied	03.03.11 16:05	Scanner

Select object(s) in the list and choose an action: Neutralize

Picture 2. Viewing scanning results.

The detected objects that may present a threat are listed in the middle of the section:

Column	Description
File	Contains the path and file name.
Details	Contains information about the threat (for example, name or type of the threat).
Action	Contains information about the action applied to the detected object. If it is empty, then no action was applied yet (see below for more information).
Date	Contains the date when the threat was detected.
Detected by	Specifies whether the threat was detected by **SpIDer Guard** or **Scanner**.

To avert detected threats

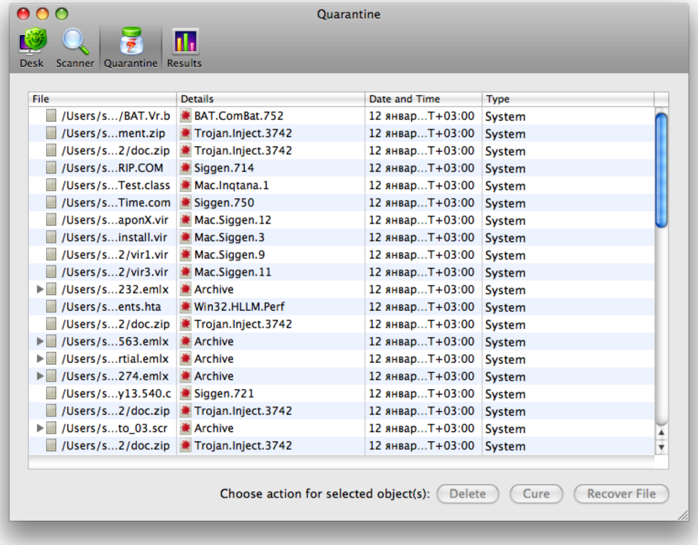
1. Select an object (hold the SHIFT key to select multiple objects).
2. Do one of the following:
   - To apply the default action as specified in the in the anti-virus preferences for the corresponding type of threats, click **Neutralize** at the bottom of the window.
   - To select a custom action, click the arrow on the **Neutralize** button.
   - Control-click an object and select a necessary action from the menu.

Managing Quarantine

Quarantine allows you to isolate detected malicious or suspicious objects that cannot be cured from the rest of the system in case you need them. Curing algorithms are being constantly improved, therefore these objects may become curable after one of the updates.

You can view and manage the contents of **Quarantine** using the **Quarantine** section of the main window (see picture below). The objects in **Quarantine** are listed in the middle of the section:

Column	Description
File	Contains the path and file name.
Details	Contains information about the threat (for example, name or type of the threat).
Date and Time	Contains the date and time when the object was moved to **Quarantine**.
Type	Specifies whether the object is stored in the system or user **Quarantine** (there is one common system **Quarantine** and separate ones for each user).



File	Details	Date and Time	Type
/Users/s.../BAT.Vr.b	BAT.ComBat.752	12 январ...T+03:00	System
/Users/s...ment.zip	Trojan.Inject.3742	12 январ...T+03:00	System
/Users/s...2/doc.zip	Trojan.Inject.3742	12 январ...T+03:00	System
/Users/s...RIP.COM	Siggen.714	12 январ...T+03:00	System
/Users/s...Test.class	Mac.Inqtana.1	12 январ...T+03:00	System
/Users/s...Time.com	Siggen.750	12 январ...T+03:00	System
/Users/s...aponX.vir	Mac.Siggen.12	12 январ...T+03:00	System
/Users/s...install.vir	Mac.Siggen.3	12 январ...T+03:00	System
/Users/s...2/vir1.vir	Mac.Siggen.9	12 январ...T+03:00	System
/Users/s...2/vir3.vir	Mac.Siggen.11	12 январ...T+03:00	System
▶ /Users/s...232.emlx	Archive	12 январ...T+03:00	System
/Users/s...ents.hta	Win32.HLLM.Perf	12 январ...T+03:00	System
/Users/s...2/doc.zip	Trojan.Inject.3742	12 январ...T+03:00	System
▶ /Users/s...563.emlx	Archive	12 январ...T+03:00	System
▶ /Users/s...rtial.emlx	Archive	12 январ...T+03:00	System
▶ /Users/s...274.emlx	Archive	12 январ...T+03:00	System
/Users/s...y13.540.c	Siggen.721	12 январ...T+03:00	System
/Users/s...2/doc.zip	Trojan.Inject.3742	12 январ...T+03:00	System
▶ /Users/s...to_03.scr	Archive	12 январ...T+03:00	System
/Users/s...2/doc.zip	Trojan.Inject.3742	12 январ...T+03:00	System

Picture 3. List of Quarantine.

To process objects in Quarantine

1. Select an object (hold the SHIFT key to select multiple objects).
2. Click the necessary button below the table:
   - Click **Delete** to completely remove the file from the file system.
   - Click **Cure** for another attempt to cure the file.
   - Click **Recover File** to move the file back to the place in the file system where it was moved from.

In the **Quarantine** section of the anti-virus preferences, you can specify a quarantine period to store objects before they will be deleted from the system completely and set the maximum size for **Quarantine**.

To configure Quarantine

In the application menu, click **Preferences** and select **Quarantine** in the left part of the window.

Configuring Schedules

Scheduler is used to set up schedules for automatic scanning and updating. It is configured via the **Scanner** and **Update** sections of the anti-virus preferences.

To configure scheduled scans

1. In the application menu, click **Preferences**, select **Scanner** and open the **Scheduler** tab.
2. Select the checkbox at the top and specify the time and interval between scanning sessions in days.

3. Select the scan mode:
   - To check only the most vulnerable system objects, select **Express**.
   - To perform full scans of the entire file system, select **Full**.
   - To specify manually which files and folders that you want to check, select **Custom**.

To configure scheduled updates

1. In the application menu, click **Preferences** and select **Update** in the left part of the window.
2. Select one of the following options:
   - To schedule update with the recommended default interval, select **Update automatically**.
   - To specify an interval for updating, select **Update every**.
   - To disable automatic updates, select **Do not update**. When operating in this mode, remember to manually update **Dr.Web for Mac OS** regularly.

Configuring Automatic Actions

Dr.Web for Mac OS can apply actions automatically when various threats are detected and not user interference is necessary. You can set different automatic reaction for **Scanner** and **SpIDer Guard**.

To configure automatic actions

1. To open automatic reaction settings for **Dr.Web for Mac OS** components, do one of the following:
   - To configure automatic actions for **Scanner**, in the application menu, click **Preferences**, select **Scanner** and open the **Actions** tab.
   - To configure automatic actions for **SpIDer Guard**, in the application menu, click **Preferences**, select **SpIDer Guard** and open the **Actions** tab.
2. Select necessary action for each type of threats.

> The default automatic actions are optimal for most uses. Do not change them unnecessarily.
>
> By default, all **SpIDer Guard** settings are locked in order to prevent anyone without administrative privileges from changing these settings. To unlock them, select the **SpIDer Guard®** section of the anti-virus preferences and click the icon of a lock at the bottom of the window.

Excluding Files from Scanning

You can make up a list of files and folders that should be excluded from scanning. You can set different exclusions for **Scanner** and **SpIDer Guard**.

To configure exclusions

1. To open exclusion settings for **Dr.Web for Mac OS** components, do one of the following:
    - To configure exclusions for **Scanner**, in the application menu, click **Preferences**, select **Scanner** and open the **Exclusions** tab.
    - To configure exclusions for **SpIDer Guard**, in the application menu, click **Preferences**, select **SpIDer Guard** and open the **Exclusions** tab.

    By default, the **Quarantine** folders are excluded from scans of both components, because they are used to isolate detected threats and, as access to it is blocked, there is no use scanning it.

2. If necessary, modify notification the list of exclusions:
    - To add a file or folder to the list, click the + button and select the object.
    - To exclude archives of all types from scanning, select **Do not check archives**.

- For **SpIDer Guard**, you can also specify a time limit for scanning one file, so the resident monitor does not "hang up" scanning corrupted files.
- For **Scanner**, you can also configure displaying of unchecked files in the scan results.

The default exclusions settings are optimal for most uses. Do not change them unnecessarily.

By default, all **SpIDer Guard** settings are locked in order to prevent anyone without administrative privileges from changing these settings. To unlock them, select the **SpIDer Guard®** section of the anti-virus preferences and click the icon of a lock at the bottom of the window.

Configuring Notifications

Dr.Web for Mac OS can notify you about various events that may occur during its operation. There are two types of notifications:

- On-screen messages displayed by **SpIDer Guard**.
- Sound alerts that are used both by **Scanner** and **SpIDer Guard**.

To configure Scanner notifications

1. In the application menu, click **Preferences**, select **Scanner** and open the **Sounds** tab.
2. Sound alerts are enabled by default. To disable or enable sound alerts, clear or select the **Use sound alerts** checkbox.
3. If necessary, modify settings for text notifications:
    - Limit the time interval during the day when you want to receive sound alerts. At any other time, scans will be performed in silent mode.
    - In the list of events, select checkboxes next to events that should be accompanied by a sound alert.

- To assign a particular sound for an event, select the event and pick a sound from the **Sound** list. To add another sound to the list, click **Choose** and select a sound file.

To configure SpIDer Guard notifications

1. In the application menu, click **Preferences**, select **SpIDer Guard** and open the **Notifications** tab.
2. Notification messages are enabled by default. To disable or enable on-screen notifications, clear or select the **Show notifications** checkbox.
3. If necessary, modify settings for text notifications:
   - Select the **Remember position** checkbox if you want to display messages at that position on the screen where you moved the last notification.
   - Use the slider to set the time for messages to remain on the screen after they are reviewed. The unread messages remain on the screen until you read them.
4. Sound alerts are enabled by default. To disable to enable sound alerts, clear or select the **Use sound alerts** checkbox.
5. If necessary, modify notification settings:
   - Limit the time interval during the day when you want to receive sound alerts. At any other time, scans will be performed in silent mode.
   - In the list of events, select checkboxes next to events that should be accompanied by a sound alert.
   - To assign a particular sound for an event, select the event and pick a sound from the **Sound** list. To add another sound to the list, click **Choose** and select a sound file.

By default, all **SpIDer Guard** settings are locked in order to prevent anyone without administrative privileges from changing these settings. To unlock them, select the **SpIDer Guard®** section of the anti-virus preferences and click the icon of a lock at the bottom of the window.

Configuring Operation Mode

If necessary, you can use your installation of **Dr.Web for Mac OS** to connect to corporate networks managed by **Dr.Web Control Center** or to access **Dr.Web® AV-Desk** anti-virus service of your IT provider. To operate in such central protection mode, you do not need to install additional software or uninstall **Dr.Web for Mac OS**.

By default, **Dr.Web for Mac OS** mode settings are locked in order to prevent anyone without administrative privileges from changing these settings. To unlock them, select the **Mode** section of the anti-virus preferences and click the icon of a lock at the bottom of the window.

To use central protection mode

1. Contact an anti-virus network administrator of your company or IT provider for a public key file and parameters of connection to the central protection server.
2. In the application menu, click **Preferences** and select **Mode**.
3. To connect to central protection server of your company or IT provider, select the **Use central protection server** checkbox.

   In the central protection mode, the option of manual start and configuring updates is blocked. Some features and settings of **Dr.Web for Mac OS**, particularly concerning the constant protection and on-demand scanning, may be modified and blocked for compliance with the company security policy or according to the list of purchased services. A key file for operation in this mode is received from central protection server. Your personal key file is not used.

4. On switching to the central protection mode **Dr.Web for Mac OS** restores parameters of the previous connection. If you are connecting to the server for the first time or connection parameters have changed, do the following:
   - Enter the IP address of the central protection server provided by administrator of anti-virus network.

- Enter the port number that is used to connect to the server.
- Drag the public key file to the settings window, or double-click the public key area and browse to select the file.
- As an option, enter the authentification parameters: station ID, which is assigned to your computer for registration at the server, and password. The entered values are saved with Keychain system. Therefore, you need not enter them again when reconnecting to the server.

To use standalone mode

1. In the application menu, click **Preferences** and select **Mode**.
2. To switch to the standalone mode, clear the **Use central protection server** checkbox.

   On switching to this mode, all settings of **Dr.Web for Mac OS** are unlocked and restored to their previous or default values. You can once again access all features of anti-virus.

3. For correct operation in standalone mode, **Dr.Web for Mac OS** requires a valid personal key file. The key files received from central protection server cannot be used in this mode. If necessary, you can receive or update a personal key file with License Manager.

Using License Manager

License Manager is a component that simplifies management of your key files (see License Key File). You should install a key file after installation because it unlocks updating, constant protection and on-demand scanning features. If you have not received a key file or it has expired, you can use **License Manager** to get a new one.

To open License Manager

In the application menu, click **License Manager**.

The **License Manager** window displays details of your current key file and provides you the following license management options:

Option	Description
Get new license	Allows you to license the use of **Dr.Web for Mac OS** or renew an expired license. You can renew your license if necessary.
My Dr.Web	Opens your personal page of the official **Doctor Web** website with the default Internet browser. This page provides you with information on your license including usage period and serial number, allows to renew the license, contact Technical Support, etc.
Technical support	Opens the Technical Support page on the official **Doctor Web** website.

Registering Anti-virus

License Manager helps you register the use of **Dr.Web for Mac OS** by installing a previously received license from file, or obtaining a new license via the Internet using the registration procedure.

To start registration from **License Manager**, click **Get new license**. When running **Dr.Web for Mac OS** for the first time, the registration procedure start automatically.

⚠ By default, the key file should be located in the /Library/Application Support/DrWeb/keys/ folder. **Dr.Web for Mac OS** verifies the file regularly. Do not edit or otherwise modify the file to prevent the license from compromise.

If no valid license or demo key file is found or a license expires, all components are blocked until you renew the license or get a new one.

To install existing key files

1. On the first step of the procedure, select I already have a key file.
2. Select a key file. If you received the key file in an archive, you may select an archive.

   Dr.Web for Mac OS automatically switches to using the new key file.

To get a new key file

1. On the first step of the registration procedure, do one of the following:
   - If you have a registration serial number, select **Receive license key file** and click **Next**.
   - If you installed **Dr.Web for Mac OS** with demonstration purposes, select **Receive demo key file**, click **Next** and proceed to step 4.
2. Enter a serial number to receive a license key file and click **Next**.
3. If you have a previous license key file, provide it.

   If you have been a user of **Dr.Web for Mac OS** in the past and are registering a new license, you are eligible for extension of your new license for another 150 days. If you are registering a renewal license and fail to provide a previous license key file, your new license period will be reduced.

   Click **Next**.

4. To receive a key file, enter personal data (your given name, family name, and e-mail address), select the country and enter the city name. All the fields listed are obligatory and should be filled in. If you want to receive news about Doctor Web by e-mail, select the corresponding checkbox.
5. To download and install your key file, click **Next**. Usually, this procedure does not require your active participation.

If download fails, **Updater** provides you with information on the error. Check you Internet connection and try again.

It is recommended to keep the key file until it expires. If you re-install the product or install it on several computers, you will be able to use the previously registered license key file.

Subsequent Registration

If a key file is lost, you should register again. In this case, input the personal data which you provided during the previous registration. You may use a different e-mail address. In this case, the key file will be sent to the address specified.

When recovering a demo key file, you will receive the same key file as during the previous registration. Demo key files for the same computer cannot be received more often then once in 4 months.

The number of requests for a key file receipt is limited. One serial number can be registered not more than 25 times. If more requests are sent, the key file will not be delivered. In this case, to receive a lost key file, contact Technical Support describing your problem in detail, stating your personal data input during the registration and the serial number.

Dr.Web Console Scanner

Dr.Web Console Scanner provides you with the same full-featured on-demand scanning viruses as **Scanner** but has no graphical user interface. You can configure and run **Console Scanner** from the command line.

To run Console Scanner

1. To run **Console Scanner** with parameters, open a command line application such as Mac OS Terminal. When running without a scan path specified in parameters, **Console Scanner** loads **Dr.Web virus databases** and displays general information about the anti-virus, but does not start an anti-virus scan.

2. From the command line, run the command in the following format:

   /usr/local/bin/drweb [**-path=**<*scan path*> [**-path=**<*scan path*> ...]][<*parameters*>]

   Using the parameters, you can specify objects to scan and configure scanning preferences.

⚠ To use **Console Scanner**, ensure that the /usr/local/bin/ folder exists before installing **Dr.Web for Mac OS**.

Command Line Parameters

Command line parameters are separated by a white space and are prefixed with a hyphen '-'. To list all parameters, run **Console Scanner** with the **-?**, **-h** or **-help** parameters.

The **Console Scanner** parameters can be divided into the following groups:

- Scan area parameters
- Diagnostics parameters
- Action parameters
- Interface parameters

Scan Area Parameters

These parameters determine where to perform a virus scan:

Parameter	Description
-@[**+**]<*file*>	Instructs to scan objects listed in the specified file. Add a plus '+' if you do not want the list-file to be deleted when scanning completes.

Parameter	Description
	In a list-file, you can store paths to folders and files that should be scanned regularly. Each object must be specified in a separate line. If you do not provide full paths to objects, the search is performed in the **Console Scanner** folder, that is, /usr/local/bin/.
--	Instructs to read list of objects to scan from the standard input (STDIN).
-fl	Instructs to follow symbolic links to both files and folders. Links causing loops are ignored.
-path=*<path>* or **-path** *<path>*	Sets scan path. You can specify several paths in one parameter. If you do not provide full paths to objects, the search is performed in the **Console Scanner** folder, that is, /usr/local/bin/.
-sd	Sets recursive search for files to scan in subfolders.
-mask	Instructs to ignore masks for filenames.

Diagnostics Parameters

These parameters determine which types of objects to scan for viruses:

Parameter	Description
-al	Instructs to scan all objects defined by scan paths regardless of their file extension and structure. Scan paths are specified in the **-path** parameter. This parameter is opposite in effect to the **-ex** parameter.
-ex	Instructs to search scan paths for threats presented by files of certain types and ignore objects of other types. The list of file types should be specified in the **FileTypes** variable of the configuration file. The configuration file is defined by the **-ini** parameter. By default, objects with the following file extensions are scanned: EXE, COM, DLL, SYS, VXD, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, 386, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, PP?, OBJ, LIB, PIF, HLP, MD?, INI, MBR, IMG,

Parameter	Description
	CSC, CPL, MBP, SH, SHB, SHS, SHT*, CHM, REG, XML, PRC, ASP, LSP, MSO, OBD, THE*, NWS, SWF, MPP, OCX, VS*, DVB, CPY, BMP, RPM, ISO, DEB, AR?, ZIP, R??, GZ, Z, TGZ, TAR, TAZ, CAB, LHA, LZH, BZ2, MSG, EML, 7Z, CPIO. Scan paths are specified in the **-path** parameter. This parameter is opposite in effect to the **-al** parameter.
-ar[**d**|**m**|**r**][**n**]	Instructs to scan contents of archives (ARJ, CAB, GZIP, RAR, TAR, ZIP, etc.), both simple (*.tar) and compressed (*.tar.bz2, *.tbz). If you do not supplement the parameter with an additional **d**, **m** or **r** modifier, **Console Scanner** only informs you about detected malicious or suspicious files in archives. Otherwise, it applies appropriate actions to avert detected threats.
-cn[**d**|**m**|**r**][**n**]	Instructs to scan contents of files containers (HTML, RTF, PowerPoint). If you do not supplement the parameter with an additional **d**, **m** or **r** modifier, **Console Scanner** only informs you about detected malicious or suspicious files in containers. Otherwise, it applies appropriate actions to avert detected threats.
-ml[**d**|**m**|**r**][**n**]	Instructs to scan contents of mail files. If you do not supplement the parameter with an additional **d**, **m** or **r** modifier, **Console Scanner** only informs you about detected malicious or suspicious elements of mail files. Otherwise, it applies appropriate actions to avert detected threats.
-upn	Suppresses output of packer's names.
-ha	Enables heuristic analyser that help detect possible unknown threats.

Parameter	Description
For some parameters, you can use the following additional modifiers: • Add **d** to delete objects to avert the treat • Add **m** to move objects to **Quarantine** to avert the treat • Add **r** to rename objects to avert the treat (that is, replace the first character of the file's extension with '#') • Add **n** to disable output of the archive, container, mail file or packer type For more information on actions, see Fighting Computer Threats. If malicious objects are detected within complex objects such as archives, containers, packed or mail files, then the reaction is applied to the complex object as a whole, and not to the included malicious object only.	

Action Parameters

These parameters determine which actions to apply to infected (or suspicious) objects:

Parameter	Description
-cu[**d**|**m**|**r**]	Defines an action to apply to infected files and boot sectors. If you do not supplement the parameter with an additional modifier, **Console Scanner** cures infected objects and deletes incurable files (if another action is not specified in the **-ic** parameter). Otherwise, it applies appropriate action to infected curable object, and processes incurable files as specified in the **-ic** parameter.
-ic[**d**|**m**|**r**]	Defines an action to apply to incurable files. If you do not supplement the parameter with an additional modifier, **Console Scanner** only informs you about the threat.
-sp[**d**|**m**|**r**]	Defines an action to apply to suspicious files. If you do not supplement the parameter with an additional modifier, **Console Scanner** only informs you about the threat.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><b>-adw</b>[<b>d</b>|<b>m</b>|<b>r</b>|<b>i</b>]</td><td>Defines an action to apply to adware. If you do not supplement the parameter with an additional modifier, <b>Console Scanner</b> only informs you about the threat.</td></tr>
<tr><td><b>-dls</b>[<b>d</b>|<b>m</b>|<b>r</b>|<b>i</b>]</td><td>Defines an action to apply to dialers. If you do not supplement the parameter with an additional modifier, <b>Console Scanner</b> only informs you about the threat.</td></tr>
<tr><td><b>-jok</b>[<b>d</b>|<b>m</b>|<b>r</b>|<b>i</b>]</td><td>Defines an action to apply to joke programs. If you do not supplement the parameter with an additional modifier, <b>Console Scanner</b> only informs you about the threat.</td></tr>
<tr><td><b>-rsk</b>[<b>d</b>|<b>m</b>|<b>r</b>|<b>i</b>]</td><td>Defines an action to apply to potentially dangerous programs. If you do not supplement the parameter with an additional modifier, <b>Console Scanner</b> only informs you about the threat.</td></tr>
<tr><td><b>-hck</b>[<b>d</b>|<b>m</b>|<b>r</b>|<b>i</b>]</td><td>Defines an action to apply to hacktools. If you do not supplement the parameter with an additional modifier, <b>Console Scanner</b> only informs you about the threat.</td></tr>
<tr><td colspan="2">Additional modifiers indicate actions that should be applied for averting treats:
• Add <b>d</b> to delete objects.
• Add <b>m</b> to move objects to <b>Quarantine</b>.
• Add <b>r</b> to rename objects, that is, replace the first character of extension with '#'.
• Add <b>i</b> to ignore threats (available for minor threats only such as adware etc), that is, apply no action and do not list such threats in the report.
For more information on actions, see Fighting Computer Threats.
If malicious objects are detected within complex objects such as archives, containers, packed or mail files, then the reaction is applied to the complex object as a whole, and not to the included malicious object only.</td></tr>
</table>

Necessary actions may vary in particular cases. For most uses, a set of the following parameters is optimal:

- The **cu** parameter, that instructs to cure infected files and system areas without deletion, moving or renaming infected files.

- The **icd** parameter, that instructs to delete of incurable files.
- The **spm** or **spr** parameter, that to quarantine or rename suspicious files accordingly.

Interface Parameters

These parameters configure **Console Scanner** output:

Parameter	Description
-v, **-version**, **--version**	Instructs to output information about the product and scan engine versions and exit **Console Scanner**.
-ki	Instructs to output information about the license and its owner (in UTF8 enclоding only).
-go	Instructs to run **Console Scanner** in batch mode when all questions implying answers from a user are skipped and all decisions implying a choice are taken automatically. This mode is useful for automatic scanning of files, for example, during a daily (or weekly) check of the hard drive.
-ot	Instructs to use the standard output (STDOUT).
-oq	Disables information output.
-ok	Instructs to list all scanned objects in the report and mark "clean" object with **Ok**.
-log=[**+**] *<path to file>*	Instructs to log **Console Scanner** operations in the specified file. The file name is mandatory to turn on logging. Add a plus '+' if you want to append the log file instead of overwriting it.
-ini=*<path to file>*	Instructs to use the specified configuration file. No configuration file is supplied with **Console Scanner** by default.
-lng=*<path to file>*	Instructs to use the specified language file. The default language is English.
-ni	Disables the use of the configuration file for setting up scanning options. **Console Scanner** is configured with parameters from the command line only.
ns	Disables interruption of scanning process including the use of interruption signals (SIGINT).

Negative Form

You can use a hyphen '-' postfix with certain parameters. Parameters if such "negative" form disable respective modes, which is useful when the mode is enabled by default or within a configuration file. The following parameters have negative form:

-ar -cu -ha -ic -fl -ml -ok -sd -sp

For the **-cu**, **-ic** and **-sp** parameters, the negative form disables any action specified with additional modifiers, that is, negative form of these parameters instruct to report on detection of infected or suspicious objects, but take no actions to avert threats.

The **-al** and **-ex** parameters have no negative for, but cancel one another.

If several alternative parameters are used in the command line, the last of them takes effect.

Example

When **Console Scanner** is launched with the following command, the heuristic analyzer (enabled by default) is disabled during scanning:

drweb -path=<*scan path*> **-ha-**

Default Parameters

By default, that is, when no configuration file and other parameters apart from scan paths are specified, **Console Scanner** starts with the following parameters:

-ar -al -ha -fl- -ml -sd

This set configures scanning of all files, archives, packed files and mailboxes regardless of their file structure and extension, instructs to scan subfolders and ignore symbolic links, and enables heuristic analysis for detection of possible unknown threats. When running with default settings, **Console Scanner** reports on detected threats, but takes no other action to avert them (that is, it does not cure infected objects or delete incurable files etc). To configure **Console Scanner** to apply necessary actions automatically, specify action parameters explicitly.

Default settings are sufficient for everyday diagnostics of your system. If some of default parameters are not necessary in a particular case, you can disable them by specifying their "negative" form manually when running **Console Scanner**, that is, with a hyphen '-' postfix. The "negative" form of command line parameters is described above.

⚠ Disabling scan of archives and packed files decreases antivirus protection significantly, because viruses are often distributed as archives (especially, self-extracting) in e-mail attachments. Microsoft® Office documents which are potentially susceptible to infection with macro viruses (Microsoft® Word, Microsoft® Excel, etc) are also e-mailed in archives and containers.

However, when constant antio-virus protection with **SpIDer Guard** is enabled, then, even if a file within an archive or e-mail attachment is infected, the residet guard will immediately detect and avert the threat when you try to extract archived files or download the attachment, so the virus will not be able to affect other files or spread within your computer or network.

Excluding complex files from scanning may considerably reduce scan time.

Appendices

Appendix A. Types of Computer Threats

Herein, the term "threat" is defined as any kind of software potentially or directly capable of inflicting damage to a computer or network and compromising the user's information or rights (that is, malicious and other unwanted software). In a wider sense, the term "threat" may be used to indicate any type of potential danger to the security of the computer or network (that is, vulnerabilities that can result in hacker attacks).

All of the program types stated below have the ability to endanger the user's data or confidentiality. Programs that do not conceal their presence (e.g. spam distribution software and various traffic analyzers) are usually not considered as computer threats, although they can become threats under certain circumstances.

In **Doctor Web** classification, all threats are divided according to the level of severity into two types:

- **Major threats** – classic computer threats that may perform destructive and illegal actions in the system on their own (erase or steal important data, crash networks, etc.). This type of computer threats consists of software that is traditionally referred to as malware (malicious software), that is, viruses, worms and Trojans.
- **Minor threats** – computer threats that are less dangerous than major threats, but may be used by a third person to perform malicious activity. Also, mere presence of minor threats in the system indicates its low protection level. Among IT security specialists this type of computer threats is sometimes referred to as grayware or PUP (potentially unwanted programs) and consists of the following program types: adware, dialers, jokes, riskware, hacktools.

Major threats

Computer Viruses

This type of computer threats is characterized by the ability to implement its code into other objects. Such implementation is called infection. In most cases, the infected file becomes a virus carrier itself and the implemented code does not necessarily match the original. Most viruses are intended to damage or destroy data in the system.

In **Doctor Web** classification, viruses are divided by the type of objects which they infect:

- **File viruses** infect files of the operating system (usually executable files and dynamic libraries) and activate upon launching of the infected file.
- **Macro-viruses** are viruses that infect documents used by Microsoft® Office and some other applications supporting macro commands (usually, written in Visual Basic). Macro commands are a type of implemented programs (macros) written in a fully functional programming language. For instance, in Microsoft® Word macros can automatically initiate upon opening (closing, saving, etc.) a document.
- **Script viruses** are created using script languages and usually infect other scripts (e.g. service files of an operating system). They are also able to infect other file formats that allow execution of scripts and thus take advantage of scripting vulnerabilities in Web applications.
- **Boot viruses** infect boot records of diskettes and partitions or master boot records of fixed disks. They require very little memory and remain ready to continue performing their tasks until a system roll-out, restart or shut-down occurs.

Most viruses have some kind of protection against detection. Protection methods are being constantly improved and ways to overcome them are constantly being developed. All viruses may also be classified according to the type of protection that they use:

- **Encrypted viruses** cipher their code upon every infection to hamper their detection in a file, boot sector or memory. All copies of such viruses contain only a small common code fragment (the decryption procedure) that can be used as a virus signature.

- **Polymorphic viruses** also encrypt there code, but besides that they also generate a special decryption procedure that is different in every copy of the virus. This means that such viruses do not have byte signatures.
- **Stealth viruses** perform certain actions to disguise their activity and thus conceal their presence in an infected object. Such viruses gather the characteristics of an object before infecting it and then plant these “dummy” characteristics that mislead the scanner searching for modified files.

Viruses can also be classified according to the programming language in which they are written (in most cases, it is Assembler, high-level programming languages, script languages, etc.) or according to affected operating systems.

Computer Worms

Worms have become a lot more widespread than viruses and other types of computer threats recently. Like viruses, they are able to reproduce themselves and spread their copies, but they do not infect other programs and files (that is, they do not need host files to spread). A worm infiltrates a computer from a worldwide or local network (usually via an attachment to an e-mail) and distributes its functional copies to other computers in the network. It can begin distributing itself either upon a user’s action or in an automatic mode choosing which computers to attack.

Worms do not necessarily consist of only one file (the worm’s body). Many of them have an infectious part (the shellcode) that loads into the main memory (RAM) and then downloads the worm’s body as an executable file via the network. If only the shellcode is present in the system, the worm can be deleted by simply restarting the system (at which the RAM is erased and reset). However, if the worm’s body infiltrates the computer, then only an anti-virus program can cope with it.

Worms have the ability to cripple entire networks even if they do not bear any payload (i.e. do not cause any direct damage) due to their intensive distribution.

In **Doctor Web** classification, worms are divided by the method of distribution:

- Net worms distribute their copies via various network and file-sharing protocols.
- Mail worms spread themselves using e-mail protocols (POP3, SMTP, etc.).
- Chat worms use protocols of popular messengers and chat programs (ICQ, IM, IRC, etc.).

Trojan Programs (Trojans)

This type of computer threats cannot reproduce itself or infect other programs. A Trojan substitutes a program that is used a lot and performs its functions (or imitates its operation). At the same time, it performs some malicious actions in the system (damages or deletes data, sends confidential information, etc.) or makes it possible for hacker to access the computer without permission, for example, to harm the computer of a third party.

A Trojan’s masking and malicious facilities are similar to those of a virus. A Trojan may even be a component of a virus. However, most Trojans are distributed as separate executable files (through file-exchange servers, removable data carriers or e-mail attachments) that are launched by users or system tasks.

It is very hard to classify Trojans due to the fact that they are often distributed by viruses or worms and also because many malicious actions that can be performed by other types of threats are ascribed to Trojans only. Here are some Trojan types which are distinguished as separate classes in **Doctor Web**:

- **Backdoors** are Trojans that make it possible for an intruder to log on into the system or obtain privileged functions bypassing any existing access and security measures. Backdoors do not infect files, but they write themselves into the registry modifying the registry keys.

- **Rootkits** are used to intercept system functions of an operating system in order to conceal themselves. Besides, a rootkit can conceal processes of other programs (e.g. other threats), registry keys, folders and files. It can be distributed either as an independent program or as a component of another malicious program. There are two kinds of rootkits according to the mode of operation: User Mode Rootkits (UMR) that operate in user mode (intercept functions of the user mode libraries) and Kernel Mode Rootkits (KMR) that operate in kernel mode (intercept functions on the level of the system kernel, which makes it harder to detect).
- **Keyloggers** are used to log data that users enter by means of a keyboard. The aim of this is to steal personal information (i.e. network passwords, logins, credit card data, etc.).
- **Clickers** redirect hyperlinks to certain addresses in order to increase traffic of Web sites or perform DDoS attacks.
- **Proxy Trojans** provide anonymous Internet access through a victim's computer.

Trojans may also perform other malicious actions besides those stated above, for example, change the start page in a Web browser or delete certain files. However, other actions can also be performed by other types of threats (viruses and worms).

Minor Threats

Hacktools

Hacktools are programs designed to assist the intruder with hacking. The most common among them are port scanners that detect vulnerabilities in firewalls and other components of computer protection system. Besides hackers, such tools are used by administrators to check security of their networks. Occasionally, common software that can be used for hacking and various programs that use social engineering techniques are designated as among hacktools as well.

Adware

Usually, this term refers to a program code implemented into freeware programs that force display of advertisements to users. However, sometimes such codes can be distributed via other malicious programs and show advertisements in Web browsers. Many adware programs operate with data collected by spyware.

Jokes

Like adware, this type of minor threats can not be used to inflict any direct damage to the system. Joke programs usually just generate messages about errors that never occurred and threaten to perform actions that will lead to data loss. Their purpose is to frighten or annoy users.

Dialers

These are special programs that are designed to scan a range of telephone numbers and find those where a modem answers. These numbers are then used to mark up the price of telephoning facilities or to connect the user to expensive telephone services.

Riskware

These programs were not intended as computer threats, but can potentially cripple or be used to cripple system security due to certain features and, therefore, are classified as minor threats. Riskware programs are not only those that can accidentally damage or delete data, but also ones that can be used by crackers or some malicious programs to do harm to the system. Among such programs are various remote chat and administrative tools, FTP-servers, etc.

Suspicious Objects

These are possible computer threats detected by the heuristic analyzer. Such objects can potentially be any type of threat (even unknown to IT security specialists) or turn out safe in case of a false detection.

Suspicious objects should be sent for analysis to the **Dr.Web Virus Laboratory**.

Appendix B. Fighting Computer Threats

There are many methods of detecting and averting computer threats. All **Dr.Web products** combine these methods for the most reliable protection of computers and networks using flexible user-friendly settings and comprehensive approach towards security assurance.

Detection methods

Signature checksum scanning

This method is a type of signature analysis. A signature is a continuous finite byte sequence unique to a certain computer threat. If a signature from the virus database is found in a program's code which is being scanned, then a detection occurs.

Signature checksum scanning implies comparison of signature checksums rather then signatures themselves. This helps to reduce the size of the virus databases considerably and maintain reliability of traditional signature analysis.

Execution emulation

The program code execution emulation method is used to detect polymorphic and encrypted viruses in cases when implementation of signature checksum analysis is impracticable or extremely difficult (due to impossibility of extracting a reliable signature from a sample). This is how the method is performed: an emulator, which is a software model of the CPU, simulates execution of an analyzed code sample; instructions are executed in protected memory space (emulation buffer) and are not passed on to the CPU for actual execution; when an infected file is processed by the emulator, the result is a decrypted virus body, which can be easily defined via signature checksum analysis.

Heuristic analysis

Heuristic analysis is used to detect newly created unknown computer threats, whose byte signatures have not yet been added to virus databases. Operation of the heuristic analyzer is based on defining and calculating the summary weight of certain features which are either typical for computer threats or, on the contrary, very rarely found in them. These features are characterized by their weight (a figure which defines the importance of a feature) and sign (positive sign means that the feature is typical for computer threats; negative means that the feature is not relevant for them). If the sum of these features for an object exceeds a certain operation threshold, the heuristic analyzer concludes that the object may be a threat and defines it as suspicious.

As with other hypothesis checking systems, heuristic analysis assumes the possibility of false positives (that is, type I errors when a threat is overlooked) and false negatives (that is, type II errors of a false detection).

Origins Tracing™

Origins Tracing™ is a unique non-signature threat detection algorithm developed by **Doctor Web** and used only in **Dr.Web products**. Combined with traditional signature-based scanning and heuristic analysis, it significantly improves detection of unknown threats. The .Origin extension is added to names of objects detected using the **Origins Tracing** algorithm.

Actions

To avert computer threats, **Dr.Web products** use a number of actions that can be applied to malicious objects. A user can leave the default settings, configure which actions to apply automatically, or choose actions manually upon every detection. Below is a list of possible actions:

- **Cure** is an action that can only be applied to major threats (viruses, worms and Trojans). It implies deletion of malicious code from infected objects as well as recovery of their structure and operability to the state in which it was before the infection if possible. Sometimes malicious objects are made of malicious code only (for example, Trojans or functional copies of computer worms) and for such objects to cure the system means to remove the whole object completely. Not all files infected by viruses can be cured, but curing algorithms evolve all the time.
- **Quarantine** (Move to Quarantine) is an action when the detected threat is moved to a special folder and isolated from the rest of the system. This action is preferable in cases when curing is impossible and for all suspicious objects. It is recommended to send copies of such files to the **Dr.Web Virus Laboratory** for analysis.
- **Delete** is the most effective action for averting computer threats. It can be applied to any type of computer threat. Note that deletion will sometimes be applied to certain objects for which the Cure action was selected. This will happen in cases if the object consists of only malicious code and have no useful information (for example, curing a computer worm implies deletion of all its functional copies).
- **Rename** is an action when the extension of an infected file is changed according to a specified mask (by default, the fist character of the extension is replaced with #). This action may be appropriate for files of other operating systems (such as MS-DOS® or Microsoft® Windows®) detected heuristically as suspicious. Renaming helps to avoid accidental startup of executable files in these operating systems and therefore prevents infection by a possible virus and its further expansion.
- **Ignore** is an action applicable to minor treats only (that is, adware, dialers, jokes, hacktools and riskware) that instructs to skip the threat without performing any action or displaying information in report.
- **Report** means that no action is applied to the object and the treat is only listed in results report.

Appendix C. Contacting Support

Support is available to customers who have purchased a commercial version of **Dr.Web** products. Visit **Doctor Web Technical Support** website at http://support.drweb.com/.

If you encounter any issues installing or using company products, take advantage of the following **Doctor Web** support options:

- Download and review the latest manuals and guides at http://download.drweb.com/
- Read the frequently asked questions at http://support.drweb.com/
- Look for the answer in Dr.Web knowledge database at http://wiki.drweb.com/
- Browse Dr.Web official forum at http://forum.drweb.com/

If you have not found solution for the problem, you can request direct assistance from **Doctor Web Technical Support** by filling in the web-from in the corresponding section of the support site at http://support.drweb.com/.

For regional office information, visit the **official Doctor Web website** at http://company.drweb.com/contacts/moscow.

Appendix D. Central Anti-virus Protection

Solutions for central protection from **Doctor Web** help automate and simplify configuring and managing information security of computers within logical structures (for example, company computers that access each other from both inside and outside of company's local networks). Protected computers are united in one anti-virus network which security is monitored and managed from central server by administrators. Connection to centralized anti-virus systems guarantees high level of protection while requiring minimum efforts from end-users.

Logical Structure of Anti-virus Networks

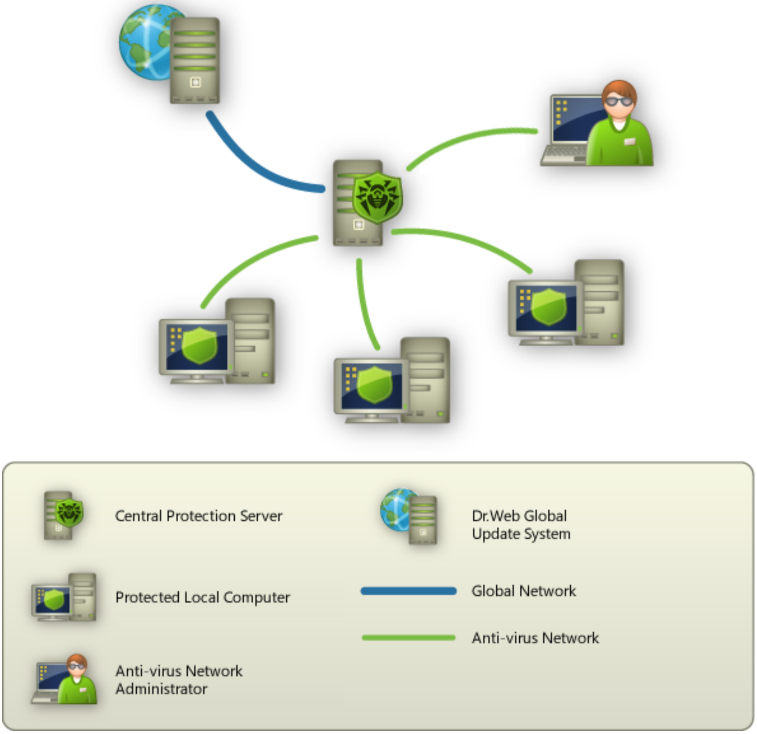
Solutions for central protection from **Doctor Web** use client-server model (see picture below).

Workstations and servers are protected by *local anti-virus components* (agents, or clients; herein, **Dr.Web for Mac OS**) installed on them, which provides for anti-virus protection of remote computers and ensures easy connection to central protection server.

Local computers are updated and configured from *central server*. The stream of instructions, data and statistics in the anti-virus network goes also through the central protection server. The volume of traffic between protected computers and the central server can be quite sizeable, therefore solutions provide options for traffic compression. To prevent leak of sensitive data or substitution of software downloaded onto protected computers, encryption is also supported.

All necessary updates are downloaded to central protection server from **Dr.Web Global Update System** servers.

Local anti-virus components are configured and managed from central protection server according to commands from *anti-virus network administrators*. Administrators manage central protection servers and topology of anti-virus networks (for example, validate connections to central protection server from remote computers) and configure operation of local anti-virus components when necessary.


Central Protection Server
Dr.Web Global Update System
Protected Local Computer
Global Network
Anti-virus Network
Anti-virus Network Administrator

Picture 4. Logical structure of anti-virus networks.

Local anti-virus components are not compatible with other anti-virus software including versions of **Dr.Web anti-virus solutions** that do not support operation in central protection mode (i.e. **Dr.Web® Anti-virus for Mac OS X** version 5.0). Installing two anti-virus programs on one computer may lead to system crash and loss of important data.

Central Protection Solutions

Dr.Web® Enterprise Security Suite

Dr.Web® Enterprise Security Suite is a complex solution for corporate networks of any size that provides reliable protection of workstations, mail and file servers from all types of modern computer threats. This solution also provides diverse tools for anti-virus network administrators that allow them to keep track and manage operation of local anti-virus components including components deployment and update, network status monitoring, statistics gathering, and notification on virus events.

Dr.Web® AV-Desk Internet Service

Dr.Web® AV-Desk is an innovative Internet service created by **Doctor Web** for providers of various types of Internet services. With this solution, providers can deliver information security services to home customers and companies providing them with a selected package of services for protection from viruses, spam and other types of computer threats for as long as is necessary. Services are provided online.

For more information on **Dr.Web® AV-Desk** Internet service, visit the official **Doctor Web** Web site at http://www.av-desk.com.

Index

Index

Index